IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MICHIGAN SOUTHERN DIVISION

DAVID ANGEL SIFUENTES III,
Plaintiff,

CASE NO.

HON.

V.

NATIONAL PUBLIC DATA,
Defendant.
_____/

COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

INTRODUCTION

1. Plaintiff, David Angel Sifuentes III ("Plaintiff"), a citizen of Gradn Rapids, Michigan, brings this action against Defendant, National Public Data ("Defendant"), a citizen and headquartered and incorporated in Coral Springs, Florida corporation, for damages and injunctive relief arising from Defendant's negligent and unlawful conduct in failing to protect Plaintiff's sensitive personal information, resulting in a massive data breach.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332, as there is complete diversity of citizenship between the parties and the amount in controversy exceeds $75,000, exclusive of interest and costs.

3. This Court has personal jurisdiction over Defendant because Defendant conducts business in the State of Michigan, and the claims in this lawsuit arise out of Defendant's business activities in Michigan. Defendant purposefully availed itself of the privilege of

conducting business in Michigan, and it is reasonably foreseeable that Defendant could be haled into court in Michigan for claims arising out of its business activities in the state.

4. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b), as a substantial part of the events or omissions giving rise to the claim occurred in this District, and Defendant is subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

5. On or about August 29, 2024, Plaintiff discovered through his identity theft protection service that his personal information had been exposed on the dark web due to a data breach.

6. Plaintiff's personal information exposed in the breach included his city, first and last name, postal code, county, state, Social Security number, address, password, and user ID.

7. Defendant has confirmed that it suffered a massive data breach involving Social Security numbers and other personal data on millions of Americans. The breach occurred in late December 2023, with potential leaks of certain data in April 2024 and summer 2024.

8. The breached data included names, email addresses, phone numbers, mailing addresses, and Social Security numbers.

9. The breach involved 2.9 billion records, including names, addresses, Social Security numbers, and relatives, dating back at least three decades.

10. The cybercriminal group USDoD accessed Defendant's network and stole unencrypted personal information. The group then posted a database containing the information on the dark web, seeking to sell it for $3.5 million.

11. Defendant failed to implement adequate security measures to protect Plaintiff's personal information, resulting in the data breach.

12. Defendant's failure to protect Plaintiff's personal information constitutes a breach of its duty of care to Plaintiff.

13. As a result of the data breach, Plaintiff has suffered and continues to suffer damages, including but not limited to:

- Increased risk of identity theft and fraud
- Emotional distress and anxiety
- Loss of time and money spent mitigating the effects of the breach
- Loss of privacy

CAUSES OF ACTION

Count I: Bailment

14. Plaintiff entrusted his personal information to Defendant for the purpose of Defendant providing background check services.

15. A bailment relationship was created, imposing a duty on Defendant to exercise reasonable care in safeguarding Plaintiff's personal information. (*Eley v. Burrows*, 130 Mich. App. 778 (1983)).

16. Defendant breached its duty of care by failing to implement adequate security measures to protect Plaintiff's personal information.

17. As a result of Defendant's breach of duty, Plaintiff's personal information was exposed in the data breach, causing Plaintiff damages.

Count II: Conversion

18. Plaintiff's personal information is Plaintiff's property.

19. Defendant exercised unauthorized control over Plaintiff's personal information by failing to protect it from the data breach. This constitutes conversion as it is a distinct act of dominion wrongfully exerted over Plaintiff's personal property. (*Foremost Ins. Co. v. Allstate Ins. Co.*, 439 Mich. 378 (1992)).

20. Defendant's unauthorized control over Plaintiff's personal information deprived Plaintiff of his right to possess and control his own property.

21. As a result of Defendant's conversion, Plaintiff has suffered damages.

Count III: Negligence

22. Defendant owed Plaintiff a duty of care to protect his personal information from unauthorized access and disclosure.

23. Defendant breached its duty of care by failing to implement adequate security measures to protect Plaintiff's personal information.

24. Defendant's breach of duty was the proximate cause of the data breach and Plaintiff's resulting damages. The elements of negligence - duty, breach, causation and damages are met. (*Case v. Consumers Power Co.*, 463 Mich. 1 (2000)).

Count IV: Negligent Infliction of Emotional Distress

25. Defendant's negligent conduct in failing to protect Plaintiff's personal information caused Plaintiff to suffer severe emotional distress.
26. Plaintiff's emotional distress is a foreseeable result of Defendant's negligent conduct, making Defendant liable for negligent infliction of emotional distress. (*Dalley v. Dykema Gossett PLLC*, 287 Mich. App. 296 (2009)).

Count V: Breach of Implied Contract

27. Plaintiff and Defendant entered into an implied contract whereby Defendant agreed to provide background check services to Plaintiff in exchange for Plaintiff providing his personal information.

28. The implied contract included an implied term that Defendant would exercise reasonable care in safeguarding Plaintiff's personal information. (*Featherston v. Steinhoff*, 226 Mich. App. 584 (1997)).

29. Defendant breached the implied contract by failing to protect Plaintiff's personal information from the data breach.

30. As a result of Defendant's breach of contract, Plaintiff has suffered damages.

Count VI: Breach of Fiduciary Duty

31. Defendant owed Plaintiff a fiduciary duty to protect his personal information due to the special relationship of trust and confidence between them. (*Ulrich v. Federal Land Bank of St. Paul*, 192 Mich. App. 194 (1991)).

32. Defendant breached its fiduciary duty by failing to implement adequate security measures to protect Plaintiff's personal information.

33. As a result of Defendant's breach of fiduciary duty, Plaintiff has suffered damages.

Count VII: Violation of the Michigan Consumer Protection Act

34. Defendant's failure to protect Plaintiff's personal information constitutes an unfair, unconscionable, or deceptive method, act, or practice in the conduct of trade or commerce, in violation of the Michigan Consumer Protection Act, [State law citation]. (*Nessel v. 411 Pain LLC,* 506 Mich. 1 (2020)).

Count VIII: Invasion of Privacy

35. Defendant's failure to protect Plaintiff's personal information resulted in the public disclosure of Plaintiff's private information, causing Plaintiff embarrassment, humiliation, and mental anguish. This constitutes an invasion of privacy. (*Doe v. Mills,* 212 Mich. App. 73 (1995)).

Count IX: Identity Theft

36. As a direct and proximate result of the data breach caused by Defendant's negligence, Plaintiff's personal information was exposed and made available to unauthorized individuals, increasing the risk of identity theft. Plaintiff has a reasonable fear of imminent identity theft and has incurred costs and suffered damages in an effort to mitigate and prevent such identity theft.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment against Defendant as follows:

1. **Actual damages** in the amount of $250,000.

2. **Punitive damages** in the amount of $650,000.
3. **Injunctive relief** requiring Defendant to:
    - Cease using Plaintiff's personal information.
    - Take all necessary steps to secure its servers and protect Plaintiff's personal information from further unauthorized access or disclosure.
    - Provide proof to the Court that it has replaced its servers and implemented adequate security measures to protect Plaintiff's and other consumers' personal information.
4. **Such other and further relief** as this Court deems just and proper.

Respectfully submitted,

By: _____

In Pro Se
David Angel Sifuentes III
439 More St. NE
Unit 2
Grand Rapids, MI 49503
(616) 283-5215

Dated: September 4, 2024